



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/912,174

07/24/2001

Takumi Okauc

SONYJP 3.0-191

5689

530

7590

12/06/2005

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER

LASHLEY, LAUREL L

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 12/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/912,174	Applicant(s) OKAUE, TAKUMI	
	Examiner Laurel Lashley	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 July 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 July 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☒ Certified copies of the priority documents have been received in Application No. 09/912,174.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1 – 28 have been examined.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. P2000-222124, filed on July 24, 2000.

Information Disclosure Statement

3. The information disclosure statements (IDSs) submitted on 11/14/2003 and 01/18/05 were filed after the mailing date of the application on 07/24/2001. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Objections

4. Claims 1, 9, 20, and 24 are objected to because of the following informalities:
 - Claims 1 and 9 recite “an enabling key blocks”, which combines singular (i.e. an) and plural (i.e. blocks) tenses.
 - Claims 20 and 24 contain duplicate texts “wherein the” and “wherein” respectively.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1 - 13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claims 1 and 9 recite the limitations "said enciphering keys". There is insufficient antecedent basis for this limitation in these claims.
- Claims 3 and 11 recite the limitations "said link count data". There is insufficient antecedent basis for this limitation in these claims.

Appropriate correction is required throughout the entire application.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1 – 28 rejected under 35 U.S.C. 103(a) as being unpatentable over Caronni et al. in US Patent 6,049,878 (hereinafter US '878) in view of Lotspiech in US Patent 6,609,116 (hereinafter US '116).

7. As it pertains to claims 1, 9 and 14, Caronni et al. in US '878 discloses:

an enabling key block distribution key enciphering key enciphered by an enabling key blocks containing enciphered data of renewal keys on such paths for constituting a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of devices, wherein said enabling key block also contains data of upper-rank key enciphered via lower-rank key;(see US '878: column 4, lines 23 – 38 and column 6, lines 20 – 46)

but does not teach wherein

said data processing apparatus further comprises key distribution approval data files containing header data consisting of link count key for designating the number of contents data that should be enciphered by said enciphering keys acquirable based on said enabling key

block distribution key enciphering key stored in said enabling key blocks, thereby said key distribution approval data files are stored in said memory device.

Lotspiech however does disclose:

said data processing apparatus further comprises key distribution approval data files containing header data consisting of link count key for designating the number of contents data that should be enciphered by said enciphering keys acquirable based on said enabling key block distribution key enciphering key stored in said enabling key blocks, thereby said key distribution approval data files are stored in said memory device (see US '116: column 4, lines 16 – 20).

For claims 1, 9 and 14, it would be obvious to one of ordinary skill in the art at the time of the invention to modify the methods of Caronni et al. and Lotspiech as they both use features of secure data communication within the same field of endeavor (securely communicating content data) and with the same problem sought to be solved (reducing the load incurred from distribution of communication content).

Regarding claims 15, 23 and 28 as taught by Caronni et al. in US '878, which disclose as an apparatus, method and medium respectively:

enabling key block distribution authenticating key, wherein the enabling key block distribution authenticating key is previously enciphered by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein the device is associated with one of the leaf keys, and wherein said enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys; (see US '878: column 4, lines 23 – 38 and column 6, lines 20 – 46) and

but does not disclose

wherein, the memory device stores a key distribution approval data file comprising header data, which comprises a link count key for designating a number of contents data that should be enciphered by the enciphering data acquirable from the enabling key block distribution authenticating key.

Caronni et al. however does teach:

wherein, the memory device stores a key distribution approval data file comprising header data, which comprises a link count key for designating a number of contents data that should be enciphered by the enciphering data acquirable from the enabling key block distribution authenticating key (see US '116: column 4, lines 16 – 20).

For claims 15, 23 and 28, it would be obvious to one of ordinary skill in the art at the time of the invention to modify the methods of Caronni et al. and Lotspiech as they both use features of secure data communication within the same field of endeavor (securely communicating content data) and with the same problem sought to be solved (reducing the load incurred from distribution of communication content).

As it pertains to claims 5, 13, and 14 as taught by Caronni et al. in US '878, which disclose as an apparatus, method and medium respectively:

wherein said data processing apparatus stores said key enciphering key in said memory, wherein said key enciphering key are acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device; (see US '878: column 7, lines 38 – 39 and 59 – 61)

but does not teach

whenever processing contents data stored in said memory device, said data processing apparatus judges applicability of said key enciphering key previously stored in said memory device, and then, if it is identified to be applicable, said data processing apparatus utilizes said key enciphering key previously stored in said memory device, wherein, solely in the case in which said key enciphering key is identified to be inapplicable, said data processing apparatus reads said key distribution approval data files.

Lotspiech however does disclose:

whenever processing contents data stored in said memory device, said data processing apparatus judges applicability of said key enciphering key previously stored in said memory device, and then, if it is identified to be applicable, said data processing apparatus utilizes said key enciphering key previously stored in said memory device, wherein, solely in the case in which said key enciphering key is identified to be inapplicable, said data processing apparatus reads said key distribution approval data files (see US '116: column 2, lines 4 – 12).

For claims 5, 13, and 14, it would be obvious to one of ordinary skill in the art at the time of the invention to modify the methods of Caronni et al. and Lotspiech as they both use features of secure data communication within the same field of endeavor (securely communicating content data) and with the same problem sought to be solved (controllably and securely distributing keys to legitimate devices).

As it relates to claims 19 and 27 as taught by Caronni et al. in US '878, which disclose as an apparatus and method respectively, comprising the steps of:

wherein the memory device stores a key enciphering key, wherein the key enciphering key is acquired by decoding the enabling key block distribution authenticating key contained in a key distribution approval data file having a greater count number value for the link-count key

than other key distribution approval data files stored in the memory device, (see US '878: column 7, lines 38 – 39 and 59 – 61) and

wherein the device uses the key enciphering key if it is applicable to the contents data and the other key distribution approval data files otherwise (see US '116: column 2, lines 4 – 12).

For claims 19 and 27, it would be obvious to one of ordinary skill in the art at the time of the invention to modify the methods of Caronni et al. and Lotspiech as they both use features of secure data communication within the same field of endeavor (securely communicating content data) and with the same problem sought to be solved (controllably and securely distributing keys to legitimate devices).

Regarding claims 4, 12, 18 and 26, Lotspiech in view of Caronni et al. teaches as an apparatus and method:

storing said key enciphering key in said memory wherein said key enciphering key are acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device (see US '878: column 7, lines 38 – 39 and 59 – 61).

For claims 6 and 20, Lotspiech in view of Caronni et al. teaches as apparatuses: wherein version of said enabling key block distribution key enciphering key which is enciphered and presented by said enabling key block is subject to a controlling process by way of renewing every version (see US '878: column 6, line 66 – column 7, lines 1 – 6).

As it relates to claims 7 and 21, Lotspiech in view of Caronni et al. teaches as apparatuses: wherein said data processing apparatus enciphers a plurality of leaf-keys by applying a storage

key proper to said data processing apparatus and then stores said enciphered leaf-keys in a memory means inside of said data processing apparatus, wherein said leaf-keys are respectively provided in correspondence with own leaves among a hierarchy key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses (see US '878: column 8, line 56 – column 9, lines 1 – 9).

Regarding claims 8 and 22, Lotspiech in view of Caronni et al. teaches as apparatuses: wherein a device key block is stored in a memory means of said data processing apparatus, wherein said device key block itself corresponds to an assemblage of enciphered keys comprising mutually different node keys individually enciphered in plural steps on such paths ranging from own leaves to upper-rank keys of said key tree structure based on such leaf-keys provided in correspondence with own leaves among said key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves (see US '878: column 8, line 33 – column 9, lines 1 – 9).

As for claims 2, 10, 16 and 24, Caronni et al. in view of Lotspiech teaches as apparatuses and methods: wherein said key distribution approval data files include a contents key enciphering key data obtained by enciphering contents key for enciphering processing of contents by said key enciphering key (see US '116: column 2, lines 51 – 53).

For claims 3, 11, 17 and 25, Caronni et al. in view of Lotspiech teaches as apparatuses and methods: wherein said data processing apparatus executes to update said link count data in said key distribution approval data files in correspondence with variation of the number of contents; data

that is enciphered by enciphering keys acquirable based on said enabling key block distribution key enciphering key stored in the above-cited enabling key blocks (see US '116: column 2, lines 54 -58).


Conclusion

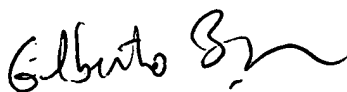
8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Laurel Lashley
Examiner
Art Unit 2132

 December 1, 2005
LLL


GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100